IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TRANSLATOR'S DECLARATION AND CERTIFICATE

APPLICANT: Bleumer

SERIAL NO.: 09/728,741 GROUP ART UNIT: 3639

FILED: December 1, 2000

TITLE: "FRANKING METHOD AND APPARATUS"

Commissioner for Patents
Box 1450
Alexandria, VA 22313-1450

S I R:

I, Charles Bullock, declare and state that I am knowledgeable in German and English, and I hereby certify that the attached translation of German Priority Application 199 58 721.3, filed in the German Patent and Trademark Office on 6 December 1999, is truthful and accurate to the best of my knowledge.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

DATE: 9 November 2005

FEDERAL REPUBLIC OF GERMANY

Priority Document concerning the Submission
of a Patent Application

File number:	199 58 721.3
Application date:	6 December 1999
Applicant/patent holder:	Francotyp-Postalia AG & Co, Birkenwerder/DE
Title:	Franking method and apparatus
IPC:	G 07 B 17/04

The attached pieces are a correct and precise reproduction of the original documents of this application.

München, the 18th of September 2000
German Patent and Trademark Office
The President
by order
[signature]

Specification

FRANKING METHOD AND APPARATUS

The invention concerns a method for machine franking of postal matter and for checking the franking according to the preamble of claim 1 as well as a method according to the preamble of claim 11. The invention moreover concerns a system for the implementation of such a method according to the preamble of claim 12 as well as a franking machine for the machine franking of postal matter according to the preamble of claim 15.

Like many other concerns, postal services in many countries of the world are increasingly conducting commerce in an electronic way, what is referred to as electronic commerce (e-commerce). Traditionally, large concerns use franking machines for franking their postal matter. Such franking machines are licensed to registered persons and require a specific connection to the postal service in order to be able to reload postage fees for the franking. In such a closed franking system, mechanical franking machines are reloaded with physical jetons (tokens) or the connections to the postal service via a special line or the telephone line exist in electronic franking machines in order to be able to download postage fees from a fee computer there. Such franking machines are only sold or leased to registered customers, and an inspection by the postal services is required at regular intervals.

Since smaller companies and offices have also in the meanwhile allocated adequate computer capacity on computers and printers is available in a simple and advantageous way, franking systems are being increasingly employed with which postage fees can be downloaded from the postal service via open networks such as the Internet and that require no special hardware with a regular inspection requirement. Given such (what are referred to as) open franking systems, a traditional PC can be used for downloading the postage fees and a standard printer can be used for printing a fee stamp on an envelope or on a label.

The U.S. Postal Service has specified a system architecture for open and closed franking systems. Such a system is known, for example, from US 5,825,893. Each user thereby has a physical, optimally breach-proof security device on which all postage fees of the user provided for the franking are stored. This security device (PSD = Postal Security Device) can be arranged inside or outside the franking machine or the computer. A fee counter and a user-associated encryption module with which the fee stamp and a further machine-readable date stamp (what are referred to as "indicia") are generated are essentially arranged in a secured device. For franking a piece postal good [sic], such an indicium is generated by the security device from the postage fee to be franked, an identification code of the security device, the sender address, the current fee counter state and, potentially, further data by means of a signature code. This indicium is then encoded in a two-dimensional bar code and printed onto the postal matter so that it can be scanned and inspected in a simple and dependable way by a checking device of the postal service. The internal postage fee counter of the franking machine is subsequently diminished by the amount of postage that has been used.

Since the users of open franking systems are not registered and the hardware that is employed is not subject to any regular inspections by the postal service, such franking systems must be protected against fraud to a more significant degree than closed franking systems. However, they must also be clearly cheaper in order to be able to penetrate into the mass market. The invention is therefore based on the object to achieve a franking method, a franking system, and a franking machine which exhibit high security against fraud given simultaneously low costs.

These objects are achieved by the methods according to claim 1 and claim 11, by the system according to claim 12 or, respectively, by the franking machine according to claim 15.

The invention is thereby based on the idea that fraud by multiple use of postage fees and/or multiple use of date stamps can be prevented in that the machine-readable date stamp applied onto the postal matter in the franking is encoded and/or designed such that it can be unambiguously differentiated from other employed date stamps. The date stamp hereby contains the imprint and/or value of an electronic coin individualized for the present franking. While standard money, for example coins and bank notes, are in fact standard payment means, the purpose of the payment, however, cannot be seen from them. Given the present invention, however, money that has been individualized for the present franking - referred to below as electronic coin - is generated with the franking, whereby this electronic coin not only contains a monetary value - such as, for example, the postage value – but moreover also contains data individualized to the franking so that a double generation of an electronic coin is precluded. The electronic coin is represented on the postal matter by a date stamp which, in addition to the postage value specification, contains further particulars identifying the electronic coin, which particulars are machine-readable. The postal service can thereby check by means of a checking device whether a date stamp has already been employed and, for example, has been cut out by a defrauder and glued onto a new letter. The multiple employment of postage fees that are stored and debited in electronic form in such franking systems can thereby be detected since it can be recognized using the date stamp whether it has been generated by means a postage that has already been consumed. Insofar as the originator of the date stamp is contained in the date stamp (in non-manipulable (encrypted) form), the defrauder can be identified in this case. In both instances, the postal matter franked with such fraudulent means can be precluded from further conveyance.

Compared to known solutions, the inventive solution exhibits the advantages that no additional hardware (such as a described security device) is hereby required for the storing and accounting of the postage fees and for storing a user-individual signature key and can be realized on a conventional computer as a pure software solution. Further, it is not absolutely necessary that data about the user are

contained in the date stamp, so that the user cannot be indicated from the date stamp, whereby the anonymity of the user is preserved. It is also not required that, in addition to the user and the postal service, a third person - as monitoring entity - monitors the franking event and the accounting of the postage fees online as in some known solutions; rather, a franking can ensue at any time and without intervention of such a monitoring entity. Overall, with the inventive solution a high security standard similar to as with cryptographically secure electronic payment systems is achieved.

In one embodiment of the inventive method, it is provided that the inspection ensues via comparisons of the date stamp to be inspected with used date stamps stored in a data bank. The comparison check of the date stamp to be inspected is equivalent with the comparison test of generated electronic coins. Since an individual date stamp (thus also an individual electronic coin individualizing the piece of mail) is generated for each piece of mail, this represents a simple realization of the inspection, whereby the data bank is stored in a suitable storage device in the inspection device. Since, however, data banks do not exhibit unlimited storage space in practice, the embodiment according to claim 3 is very advantageous. Each data stamp thereby comprises an expiration date, i.e. a date in the future of the date of the production of the date stamp until when the date stamp (or, respectively, the electronic coin) is valid and up to which, for example, the piece of mail is also carried. This time span can, for example, amount to a standard fourteen days for all users and all date stamps (or, respectively, electronic coins). This means that an electronic coin whose expiration has already expired as of the inspection can be separated out in a first stage of the inspection, and that only those used electronic coins need remain stored in the data bank that have been inspected in this time span calculated from the date of the inspection, thus in the last fourteen days in the example. For example, storage space in the data bank can thereby be made available again every day by erasing the date stamp or, respectively, electronic coins having the oldest inspection dates.

The development of the invention according to claim 4 represents one possibility via which an inspection for multiple employment of postage fees can ensue. The developments according to claims 5 and 6 essentially serve operating convenience, in that the user can compile the postage fee to be franked from individual postage fee units or can subdivide a larger postage fee unit into small sub-units.

In order, on the one hand, to enable he cited inspection of postage fees for multiple employment and, on the other hand, to prevent defrauders from producing their own postage fee units without paying for them, according to the development according to claim 7 an individual encoding of the postage fee units with a secret key is provided by the postal service. This encoding, which turns out differently for each postage fee unit, is also found again in the date stamp applied onto the postal matter, on date stamp a multiple usage of postal fee units can thus be detected.

According to a preferred development of the invention, the production date and production time, the franked postage fee and the addressee of the postal matter are contained in non-manipulable form in the date stamp. However, it can also be provided that other and/or further data such as, for example, the sender, his address or an expiration date for the postage fee are also contained.

For capacity reasons it can be provided that not all frankings and date stamps are inspected. It can thus be provided that the inspection is only implemented in the fashion of spot checks, that not all inspected date stamps are stored in the data bank or that a date stamp to be inspected is only compared with a part of the date stamps stored in the data bank for reasons of time. In order to nonetheless prevent that fee stamp and date stamp are separated from or cut off from a conveyed piece of mail or copied by means of a copier and simply glued or copied onto the postal matter to be franked, further postal matter data can be incorporated in the date stamp in the development of claim 9. These postal matter data can quasi-serve as an individual fingerprint of the postal matter to be franked and thus turn out

differently for each piece of mail. For example, the surface structure (surface fiber structure, roughness of the surface) of the packaging material or of the envelope or another measurable property that individualizes the individual piece of mail (such as, for example, the exact weight) can be employed as postal matter data, these being either input by the user or automatically measured in the franking by means of a measuring device integrated into the franking machine.

Proceeding from this consideration, it can also be provided according to claim 10 that these postal matter data are artificially added to the postal matter in the form of label data situated on a label. Such a label can, for example, carry a hologram or a barcode whose data are integrated in the data stamp as postal matter data. Via the measures according to claims 9 and 10, it is achieved that a date stamp must also belong to the postal matter franked therewith and not be employed for some other postal matter which comprises different postal matter data. This can be established in the inspection of the date stamp insofar as the inspection means is suitably fashioned for measuring the postal matter data of the postal matter to be inspected, and these measured postal data are then compared with the postal matter data contained in the date stamp.

The method according to claim 11, which can be executed on an individual franking machine, can be developed in embodiments like the method described above. The system specified in claims 12 through 14 for the implementation of the method according to claim 1 as well as the franking machine specified in claims 15 and 16 can also be configured in a corresponding way.

The invention is explained in greater detail in the following by way of example with reference to the drawings. Shown are:

Figure 1 the block diagram of an inventive franking system;

Figure 2 a postal good franked according to the inventive method;

Figure 3 the protocol processed to open a postal fee account;

Figure 4 the protocol processed to download a postage fee unit;

Figure 5 the protocol processed for generating a date stamp;

Figure 6 the protocol processed for detecting duplicate use of a postage fee unit. [sic]

Figure 7 shows an exemplary imprint (of a date stamp or, respectively, of an electronic coin) with a data matrix of 40 x 40 elements.

The franking and mail-carrying system shown in Figure 1 comprises a postal service 1, a franking machine 2 and a mail-carrying service 3. The postal service 1 essentially comprises a postage fee device 11 for outputting and accounting of postage fee units and an inspection device 13 for inspecting and devaluing frankings. The postage fee device 11, which need not necessarily be arranged in a post office but rather can, for example, also be localized by a third party or on the Internet, provides postage fee units for franking postal matter that can be purchased or electronically downloaded at any time by the user of a franking machine. The postage fee units (i.e. electronic coins) are generated by means of a device 12 upon output; the debiting and accounting ensue by means of an accounting device 15.

The franking machine 2 comprises a central unit 21 and a printer unit 22 which, in an open franking system, can be realized by a standard PC and a standard printer. The central unit 21 comprises a fee module 23 that downloads the postage fee units from the postal service, stores them and internally debits them given a franking. The storing of postage fees can, for example, thereby ensue on the hard disk of the PC, on a chip card or on another storage medium. The accounting of postage fees with the postal service usually ensues upon download of postage fees from the

postal service 1, while the internal accounting ensues upon printout of a franking. The accounting with the postal service can thereby ensue by means of a separately established debiting account, by means of credit card, by electronic payment or by cash payment. In order to protect data for the generation of the date stamp when franking a piece of mail against manipulation, a cryptographic module 24 is also provided. Finally, for print control a print control module 25 is provided which controls the printer means 22. The fee stamp and the data stamp can either be printed directly on the postal matter or can be printed on a label to be glued onto the postal matter. The franked postal matter is subsequently conveyed by a mail-carrying service 3, whereby either there or in the postal service 1 (for example in a mail collecting center) it passes through an inspection device 13 where the franking is inspected and devalued. To this end, the inspection device 13 comprises a memory device 14, wherein, in particular, used date stamps are stored with which a date stamp to be checked is compared. A connection between the postage fee device 11 and the inspection device 13 can also exist in order, for example, to keep accounts about used and devalued postage fee units and to assure that the inspection device 13 knows the encoding of postage fee units, which can change at regular time intervals.

The franking, which comprises at least one fee stamp and a date stamp in the present case and is generally referred to as "indicium", should comprise at least the franked postage fee and an electronic signature for authorization of this postage fee. Additionally, further data can be provided in order to support specific functions of the mail-carrying system. For example, the delivery address can be contained in machine-readable form in order to enable automatic mail sorting. For anonymity reasons, the identity of the sender can thereby also be omitted. The machine-readable part of the franking can, for example, be printed in the form of a two-dimensional bar code. When a franking proves valid and sufficient, the postal matter is delivered to the corresponding recipient.

Such a franking and mail-carrying system must be protected against fraud insofar as possible; fee accounts of users must be protected against unauthorized access; data protection and anonymity must be protected within certain limits, and other security demands (that should be explained in detail in the following) must be taken into consideration.

a) At any point in time, the mail-carrying system should only carry as much mail as is covered by paid fees. As a sub-criterion, the duplicate usage of postage fees should be prevented: after a user has downloaded postage fees in a value of x, he should be able to print out a maximum of fee stamps whose total value does not exceed the value x. In open franking systems, the recipient address and a time mark are usually already contained in the date stamp, so that a reuse of a franking that has already been employed is thereby largely precluded even without further cryptographic security measures. In closed franking systems in which the franking process is separate from the addressing process, such that the recipient address is usually not contained in the date stamp, copies of frankings can, however, be detected in that, as in the inventive system, frankings (i.e. the date stamp of a franking) is [sic] compared with frankings that have already been used and are stored in a data bank and is [sic] thereby inspected. When a date stamp is thereby detected a second time, the postal matter franked therewith can either be charged a punitive postage and sent back to the sender or can be precluded from mail-carrying. As a further protective measure against copying of frankings, the employment of red fluorescent ink (which can only be reproduced with difficult with conventional copiers) can be provided for the fee and/or date stamp. In order to identify a user who illegally employs a postage fee unit multiple times for franking, for example, it can also be provided that the date stamp contains data about this user in in [sic] non-manipulable form, for example the number of his postage fee account or a specific user code.

b) Insofar as it is possible using the date stamp to determine a user who illegally employs frankings and/or postage fee units multiple times, protective measures must be undertaken [sic] that a correctly behaving user is not erroneously accused of such misbehavior.

c) Frankings should not reveal whether they originate from the same user except when the sender/user wishes this. Moreover, the user identity should also not derive from the franking in order to enable the anonymous dispatching of postal matter. Thus, a linking of date stamps by comparing the users should also be prevented.

In addition to the described security demands, a franking system should also offer adequate operating convenience. After downloading postage fees in a value of x, the user should have the possibility to generate any desired fee value (maximally x). Moreover, the procedure of acquiring postage fee units and the generation of frankings should be independent of one another, such that an online connection to a postage fee means need not first be produced (as in known systems for generating a franking) in order to download a postage fee which is directly converted into a franking. The franking should thus also be possible offline and without intervention of a third party monitoring the franking and the accounting of the postage fees.

With the inventive method and the shown inventive system, the described security demands and the described operating convenience can be achieved. Due to the individual design of the date stamp such that, for example, a different type of date stamp is required every day for each addressee, the duplicate usage of frankings can be largely precluded. A defrauder who has sent a postal item to a specific recipient could employ the franking employed for this a second time only for a second sending on the same day. Since it is also provided that the date stamps are compared in the inspection device with the date stamps already used and stored in the data bank and in [sic], frankings that are employed for a second time can be

detected with high reliability. When the generation of the date stamp is fashioned such that information about the identity of the user is contained therein, this user can also be determined in case of fraud. Since a code is also contained in the date stamp from which the postage fee units employed for generating the franking can be concluded, given this inspection it can also be established whether the corresponding postage fee units has [sic] already been used earlier for generation of a franking and therefore has [sic] been consumed. Since the postage fee units can also be acquired at any time and independent of the point in time of a franking to be undertaken and can be downloaded and can be both subdivided into smaller sub-units and combined into larger units, the required operating convenience is also achieved.

In Fig. 2, a postal matter 8 (an envelope in the example) is shown with an inventive franking and addressing. This comprises an address field 81 for the addressing, an optional sender field 82 for the return address, a fee stamp 83, a date stamp 84 and a label 85. The label 85 is optional and quasi-serves as fingerprint for the piece of mail, to which end label data contained on the label are likewise contained in a non-manipulable form in the date stamp 84. It should thereby be prevented that the fee stamp 83 and the date stamp 84 are cut out or copied and glued onto another piece of mail and illegally reused. To that end, the label 85 would also have to be reused together with the date stamp 84, which label 85 can, for example, be designed such that it is destroyed upon separation and/or cannot be copied, such as, for example, holograms, watermarks, relief impressions, etc. [sic]. Moreover, the date stamp 84 can be fashioned such that it is machine-readable, the address of the addressee is contained and can be employed for machine sorting of the postal matter. In this case, the franking could also be employed only for a postal matter directed to one and the same addressee. The arrangement, size and design of the individual fields 81 through 85 can, of course, ensue differently from that shown.

To explain individual events, protocols with individual protocol steps are shown in Figures 3 through 6. To understand these protocols, which are essentially based on

the difficulty of the calculation of discrete logarithms, some of the designations and definitions employed should be explained first. The designation manner is similar to the designation manner employed in US 5,521,980, in which an electronic payment system is described and which is herewith expressly referenced in view of further explanations of the designation manner and further definitions.

It should be designated that: Z is the set of whole numbers, q is a prime number, G is a family of finite, multiplicative Abel groups G_q of the order q. Furthermore, for a given group G_q powers g^x with ($g \in G_q$ and $x \in Z$) are defined by repeated multiplication in G_q. For a given generator g of the group G_q and an element $z \in G_q$, the smallest non-negative whole number is x, insofar as it satisfies $z = g^x$, discrete logarithm of z with respect to g. If general / generators $g_1,...,g_l \in G_q$ is given, this means that tuple $(x_1,...,x_l)$ that satisfies $z = \Pi_{i=1}^{l} g_i^{x_i}$, a discrete representation of z with respect to $g_1,...,g_l$.

Families of groups G_q are used in the following that have efficient algorithms for multiplication of group elements, uniformly distributed, random selection of group elements and testing of two group elements for equality. Moreover, the calculation of discrete logarithms is difficult, i.e. not possible in polynomial time in the bit length of q. Although the last property has not hitherto been demonstrated for any family of groups, there are candidates to which these properties are ascribed after intense research over multiple decades. This is called the discrete logarithm assumption or discrete representation assumption. Both are equivalent.

Large cyclical sub-groups of the multiplicative groups Z_p^* of finite bodies of residues modulo of a large prime number p are one candidate. Here large means that p is at least 1024 bits long. Other candidates (that, however, have not been investigated as long) are families of specific elliptic curves, large sub-groups of elliptic curves to be more precise. The elliptic curves should not be super-singular and of a low family. There are concrete recommendations from, for example, the

National Institute of Standards and Technology (NIST) [NIST99] (http://csrc.nist.gov/engryption). The current state of research is that the calculation of discrete logarithms in the former candidate given a modulo length of 1024 bits is about as difficult as the calculation of discrete logarithms in the latter candidate given a curve order of approximately 160 bits. The multiplicative notation of G_q is employed below. This notation can be easily translated into the additive notation that is standard given elliptical curves, in that multiplications in G_q are replaced by addition and powers in G_q are replaced by scalar multiples of points of a curve.

The protocols shown in Figures 3 through 6 are written in the notations standard for algorithms: via a declaration and a definition. A protocol declaration that is respectively given in the first line of the Figure is composed of the formal output parameters, followed by an allocation arrow, followed by the protocol name and the formal input parameters in brackets. In order to improve the legibility, all input and output parameters of a participant are enclosed in square brackets, whereby the abbreviation of the participant (S for user, P for postage fee device) is attached to the brackets in superscript. Formal input parameters can be taken from one protocol participant alone or from all protocol participants in common. The former are called private inputs, the latter are called common inputs. A protocol definition ensues in matrix notation, whereby the actions of each participant are written in columns below one another and each column is headed by the participant name. Successive following actions of a participant can be combined into blocks.

Protocol actions are written in the standard mathematical notation with a few specific symbols. The uniformly distributed, random selection of an element from a set A and the allocation of this element to a variable a is designated with a $\in_R A$. The evaluation of an expression E and subsequent allocation of the result to a is designated with $a \leftarrow E$. H designates a pseudo-random hash function that returns a value from Z_q after input of an arbitrary binary character sequence. It is allowed to write an H with an arbitrary number of arguments. In this case, the input to H is

the concatenation of the binary representations of all arguments. Arithmetic operations are written either in G_q, i.e. multiplication mod p, or in Z_q, i.e. addition and multiplication mod q. Multiplication and exponentiation G_q are the most frequent operations in the following. This operation is written without the supplement "mod p". The addition and multiplication in Z_q respectively receives the supplement "mod q" so that it is clear in every instance which operation is meant. If a participant of a protocol sends the value of its variable a to another participant, then an arrow $\xrightarrow{a}$ designated with a points from the column of the sending participant to the column of the receiving participant (see Fig. 3 and 4). Calls of protocols or algorithms are designated in the standard notation. The expression "proceed iff P" with P as a Boolean predicate denotes that the protocol implementation only proceeds if an only if P is valid. Otherwise the protocol is ended and the participants output a corresponding error message.

In the following protocols, p designates a large prime number, q designates a large deviser of p-1 and G_q references the unambiguous sub-group of the multiplicative group of the body Z_p that has the order q. Furthermore, g_1, g_2, G, G_0 are four generators of G_q that are selected independent of one another and are uniformly distributed randomly at the system start. The postage fee device P selects a private key $x \in Z_p^*$ randomly and with uniform distribution and calculates the corresponding public key $y = g^x \bmod p$. Digital coins (also called "piece of postage" (PoP)) are tuples (A,B,σ), whereby $A, B \in G_q$ and $\sigma = (z,a,b,r)$ are a digital signature from the range $G_0 \times G_0^2 \times G_0^2 \times Z_q$.. A digital coin is valid with respect to a public key y when it satisfies the following equation:

$$verifyPoP(y, A, B(z,a,b,r)) \equiv \left(G^r = (ya_1)^c b_1 \wedge m^r = (za_2)^c b_2 \right) \qquad (1)$$

with $c = H(A,B,z,a,b)$

In their digital form, indicia or, respectively, date stamps are tuples $(A,B,(z,a,b,r)s,rcpt,d/t)$, whereby the first part $(A,B,(z,a,b,r))$ is a digital coin and the second part $(s,rcpt,d/t)$ specifies the service that can be paid with this indicium. $s \in Z_q^3$ is thereby an auxiliary value that enables the de-anonymization of the user in case of fraud, *rcpt* is the recipient and *d/t* is the date of creation and the creation time of the indicium. Further data about the source of the indicium can be added. A date stamp is valid when the following equation is satisfied:

$$verifyInd(y, A, B(z,a,b,r)s, rcpt, d/t) \equiv \left(AB \neq 1 \wedge g_1^{S_1} g_2^{S_2} G_0^{S_3} = AB^c\right) \qquad (2)$$

with $c = H(A,B,z,a,b,r,rcpt,d/t)$

A part of the protocol sequenced given the opening of a postage fee account is shown in Figure 3. Before a user *S* can open a postage fee account, he must select a private, digital identity (u1, u2) $\in Z_q^{*2}$ in a uniformly distributed and random manner and must select his associated public digital identity $I = g_1^{U_1} g_2^{U_2} \bmod p$. Subsequently, he identifies himself with respect to the postage fee device *P* (for example by means of an identification) and opens his electronic postage fee account. He employs his public digital identity *I* as an account number. As proof that *I* is his rightful public identity, he demonstrates that he knows a discrete representation of *I* with respect to the generators g_1, g_2 (namely his private digital identity (u_1, u_2)) without showing this discrete representation to the postage fee device. This occurs in the blocks 41 through 44 in an interactive way between the user *S* and the postage fee means *P*. When the postage fee device accepts the identification and the protocol is successfully run (*acc* = *True*), a new postage fee account with number *I* is opened in the name of the user *S*.

A protocol is shown in Figure 4 that is run for downloading of digital coins. A common input is the account number *I* and the public key *y* of the postage fee device. Private input of the postage fee device *P* is its private key *x*. Private input of the user *S* is his private digital identity (u_1, u_2). First, the user demonstrates that

he possesses a discrete representation of I (Block 51). The protocol is shown in Figure 3. The postage fee device and the user take the common input I and the user takes his private digital identity (u_1, u_2) as private input. The user now selects two values w_1, $w_2 \in Z_q$ in a uniformly distributed and random manner and calculates $a \leftarrow g_1^{w_1} g_2^{w_2}$. This value a is sent to the postage fee device, which subsequently selects a value c un a uniformly distributed and random manner and sends it to the user. The user responds to this with the value pair $(r_1, r_2) = (cu_1 + w_1 \bmod q, cu_2 + w_2 \bmod q)$. In the event that the value pair returned by the user satisfies the equation $g_1^{r_1} g_2^{r_2} = h^c a$, the postage fee means accepts I as the public digital identity of the user and therewith as an account number. Next, the user selects the values u, v in a uniformly distributed and random manner according to block 52. At the same time, the postage fee device selects a value t and subsequently calculates the components z,a,b, according to block 53. The postage fee device sends z, a, b to the user. The user thereupon selects further values $\omega \in Z_q^*$ and $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in Z_q^3$ in a uniformly distributed and random manner. He then successively calculates the values $/'$, z', A', B', a', b', c', c according to block 54. Next, he sends the value c to the postage fee device that replies for the value r according to block 55. Finally, the user calculates the value r' and accepts the received digital coin $(A',B',(z',a',b',r'))$ when it is valid (see Equation (1) above) with respect to the public key y of the postage fee device (see block 56). Moreover, the user stores the discrete representation α, ß of A and B for the digital coin that was received.

When the user wishes to frank a postal matter, he selects a suitable digital coin $(A,B,(z,a,b,r))$ and calculates the corresponding indicium. The recipient *rcpt* of the postal matter, the date and the time of the creation *d/t* of the indicium and, potentially, further relevant data enter into this calculation. In addition to the postage fee unit, the user must also input the corresponding, discrete representations α, ß of A or, respectively, B. Figure 5 shows the calculations that the user implements (block 61).

When a postal item franked in this way arrives at the inspection device, the indicium can be verified according to the above equation (2). It is left to the discretion of the inspection device as to what quota of passing postal matter is inspected. When a user uses a received digital coin generate more than one indicium and therewith more than one franking even though the digital coin is only fashioned for franking a single piece of mail, then the inspection means can recognize this duplicate use with due to the fact that the components *A, B* have been used in an indicium that was inspected earlier. In this case, the two indicia are designated c_1,c_2 and the corresponding *s*-components are referenced as s_1 = (s_{11}, s_{12}, s_{13}) and s_2 = (s_{21}, s_{22}, s_{23}). The inspection device can now determine the private digital identity (u_1,u_2) of the fraudulent user with the calculating steps shown in block 71 of Figure 6 and can determine the account number I = $g_1^{U_1} g_2^{U_2} \bmod p$ of the fraudulent user from this.

Given the inventive franking method and the inventive franking system, no additional hardware is required for a security device for securing and debiting postage fees; rather, the realization is possible by means of a traditional computer and printer. As a result thereof, such a system can be realized clearly more cost-effectively, for which reason the application is also of interest for a larger mass market. At the same time, however, high security demands are met. It is also possible to realize the critical method steps purely via software that can be exchanged and improved with simple means. It is also not required that each user possess his individual key pair, for example for a digital signature system. The users and the inspection device must merely know the public key of the postal service or, respectively, of the postage fee device. This, for example, can be published on an Internet page of the postal service, and the associated public certificates can be integrated in a standard web browser. In contrast thereto, each user possesses his own, individual signature key in the known solutions, which requires as a counter-move that the postal service must either administer and store the corresponding verification keys or that each date stamp must contain the

corresponding verification key and the verification certificate. When, given the known solutions, a defrauder succeeds in breaking the signature key of a security means of the user, he can arbitrarily generate frankings without risk of discovery. In contrast to this hardware protection in the known solutions which are intended to prevent the breach of the security device, a protection with cryptographic means is assured in the inventive solution. Moreover, further security demands and demands made of the operating convenience can be realized more simply and more cost-effectively in the inventive solution.

Figure 7 shows a test imprint of a date stamp with a data matrix of 40 x 40 elements, thus the smallest data set of the options cited in Table 1. The printed date stamp is machine-readable and contains the electronic coin, its value as well as its expiration date as well as further particulars that individualize the franking. The data matrix 100 can, of course, also be formed of some other element number of mx x n elements. A standard advertising imprint is shown to the left next to the printed data matrix 100.

A method for machine franking of postal matter and for inspecting the franking has been disclosed above. The inventive concept, however, can be utilized everywhere in electronic commerce (e-commerce, IE-cash systems); for example, it is possible without further measures that services such as, for example, the output of cards and tickets (theater tickets, travel tickets, etc.) can be handled by means of the invention in decentralized and open systems. If, for example, a travel ticket is generated by the user of the travel ticket himself, the travel ticket imprint contains all data of the travel ticket-individual electronic coin. Since each travel ticket is individualized, multiple employment of the travel ticket is precluded.

Claims

1. Method for machine franking of postal matter (8) and for inspecting the franking, whereby postage fees are stored debited in electronic form as electronic coins and whereby a machine-readable date stamp containing the electronic coin is applied onto the postal matter (8), whereby an individual electronic coin that can be differentiated from electronic coins generated for other pieces of mail is generated for each piece of mail, and an inspection for multiple employment of electronic coins and/or date stamps ensues on the basis of the date stamp (84) containing the electronic coin.

2. Method according to claim 1,
characterized in that the inspection ensues by comparing the electronic coin (84) to be inspected with a used electronic coin stored in a data bank (14).

3. Method according to claim 1 or 2,
characterized in that each date stamp (8) or, respectively, the electronic coin contained therein contains an (individual) expiration.

4. Method according to claim 3,
characterized in that electronic coins that have already been used and that are only valid up to a maximum expiration date are stored in the data bank (14).

5. Method according to one of the preceding claims,
characterized in that the postage fees that represent an electronic coin are stored as postage fee units, whereby each postage fee unit comprises a postal matter-individual encoding, and in that the encoding is employed in the generation of the electronic coin for a postal item (8) such that, using the date stamp (84), it can be checked whether a postage fee unit or, respectively, electronic coin has already been employed for franking postal matter.

6. Method according to claim 5,
characterized in that a plurality of postage fee units can be combined for franking a postal item (8) and/or a postage fee unit can be composed of a plurality of electronic coins.

7. Method according to one of the preceding claims,
characterized in that the electronic coin only authenticates very specific data.

8. Method according to one of the preceding claims,
characterized in that the postage fee units are divided into a plurality of sub-units, and in that the sub-units can be employed for franking different pieces of postal matter.

9. Method according to one of the preceding claims,
characterized in that the generation of the postage fee units ensues given their purchase from a postage fee device by means of a a (secret) key known only to said postage fee device.

10. Method according to one of the preceding claims,
characterized in that the creation date and creation time, the franked postage fee and/or the addressee of the postal matter (8) are contained (in non-manipulable) form in the date stamp (84) or, respectively, in the generated, electronic coin.

11. Method according to one of the preceding claims,
characterized in that postal matter data characterizing the postal matter (8), particularly postal matter data characterizing physical properties of the postal matter, are contained in the date stamp (84) or, respectively, the generated electronic coin.

12. Method according to claim 11,

characterized in that the nature and/or surface structure of the packaging material of the postal matter are employed as uniquely characteristic [sic] and/or label data located on a label (85) additionally applied to the postal matter are employed as postal matter data.

13. Method for machine franking of postal matter (8),
whereby postage fees are stored and debited in electronic form as electronic coins and whereby a machine-readable date stamp (84) containing the electronic coin is applied onto the postal matter (8), whereby an individual electronic coin (84) that can be differentiated from electronic coins generated for other pieces of postal matter is generated and applied onto the postal matter (8), and in fact in such a way that an inspection for multiple employment of electronic coins and/or date stamps is possible on the basis of the date stamp (84) containing the electronic coin.

14. System for the implementation of the method according to claim 1,
- with a franking machine (2) for the machine franking of postal matter (8) comprising a printing unit (22) for application of a machine-readable, potentially encrypted date stamp (84) onto the postal matter (8) and comprising a central unit (21) with a fee module (23) for loading, storing and debiting of postage fees, with a print control module (25) for controlling the printing unit (22), and
- with a postage fee device (11) for output of postage fee units, and
- with an inspection device (13) for inspecting the date stamp, whereby a cryptographic module for the encryption of data for the date stamp is provided which is configured such that an individual date stamp (84) differentiable from the date stamp for other pieces of mail is generated for each piece of postal matter (8), and such that the inspection device is configured for inspecting for multiple employment of postage fees and/or date stamps on the basis of the date stamp (84).

15. System according to claim 14,

characterized in that the date stamp (84) contains the information of an electronic coin and the electronic coin is individualized for each franking, such that the electronic coins of each franking also differ from one another when the same fee value is printed onto the postal matter.

16. System according to claim 14 or 15,
characterized in that the inspection device (13) comprises a memory device (14) for storing used date stamps or, respectively, used electronic coins.

17. System according to claim 16,
characterized in that the postage fee device (11) comprises an encryption device (12) (cryptography device) for encrypting postage fee units.

18. Franking machine (2) for the machine franking of postal matter (8), comprising a printing unit (22) for applying a machine-readable date stamp containing an electronic coin onto the postal matter (8), a central unit (21) with a fee module (23) for loading, storing and debiting postage fees, with a print control module (25) for controlling the printing unit (22), whereby an individual date stamp (84) differentiable from the date stamps generated for other pieces of postal matter is generated on each piece of mail (8) such that an inspection for multiple employment of postage fees and/or date stamps and/or electronic coins is possible on the basis of the date stamp (84).

19. Franking machine according to claim 18,
characterized in that the franking machine is essentially realized by a conventional computer with a conventional printer.

Abstract

The invention concerns a method for machine franking of postal matter (8) and for the inspection of the franking, whereby postage fees are stored and debited in electronic form and whereby a fee stamp (83) and a machine-readable date stamp (84) containing encrypted data are applied onto the postal matter (8). In order to design such a method more cost-effectively, whereby high security demands are met at the same time and a realization should be possible on a traditional computer with a printer without further additional hardware, it is inventively proposed that an individual date stamp (84) differentiable from the date stamps generated for other pieces of postal matter is generated for each piece of postal matter (8) and is applied onto the piece of mail (8), and that an inspection for multiple employment of postage fees and/or date stamps ensues on the basis of the date stamp (84). This inspection is preferably realized by comparing a date stamp (84) to be inspected with previously used date stamps stored in a data bank. In particular defrauders can therewith be identified who, without payment, wish to generate frankings or, respectively, employ frankings multiple times, for example by copying. The invention also concerns a system for the implementation of such a method as well as a correspondingly-fashioned franking machine.